UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/668,455	09/23/2003	Ronald W. Szeto	019959-001900US	2353

20350 7590 03/20/2009

TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER	
HO, VIRGINIA T	

ART UNIT	PAPER NUMBER
2432	

MAIL DATE	DELIVERY MODE
03/20/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/668,455	SZETO ET AL.	
	Examiner	Art Unit	
	VIRGINIA HO	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 September 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-11* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-11* is/are rejected.

7)☒ Claim(s) *5, 6, 11* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *23 September 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *October 23, 2008; January 8, 2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. The instant application having Application No. 10/668,455 filed on September 23, 2003 is presented for examination by the examiner.

2. Examiner cites particular columns and line numbers in the references as applied to the claims below for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested that, in preparing responses, the applicant fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

Drawings

3. Example IP addresses as described in the specification with reference to the drawings should be included in the Figures.

Specification

4. The disclosure is objected to because of the following informalities: *"manger"* is a misspelling of *"manager" (page 2, line 12; page 4, line 30)*.
Appropriate correction is required.

5. The disclosure is objected to because of the following informalities: "The CPU 24 is responsible for receiving the data packets from hosts of the layer 2 subnet *which directed to the obtaining access* to the management functions of the CPU 24". *(page 3, lines 2-4)*.
Appropriate correction is required.

6. The disclosure is objected to because of the following informalities: the disclosure recites "where such packets are *in* a management VLAN" *(Page 7, lines 18-19)*. However, it is unclear what "in" refers to as the packets are in transition and could either originate from devices in the management VLAN or be received in devices in the management VLAN. Appropriate correction is required.

7. The disclosure is objected to because of the following informalities: *the specification does not follow the flow chart steps shown in the description of Figure 3*. The disclosure recites *"**If the data packet was not received on the management port 316,** then the data packet is analyzed 316 to determine if it utilizes a management protocol" (page 10, line 12-13)* upon describing the condition corresponding to a "no" response to the condition block *"Is it from mgmt sbnet 310"*.
Appropriate correction is required.

8. The disclosure is objected to because of the following informalities: *inconsistent terminology*. The disclosure recites "*level* 2 subnets" *(page 4, line 10)* rather than "layer 2 subnets" as previously mentioned.
Appropriate correction is required.

Claim Objections

9. Claim 5 is objected to because of the following informalities: *grammatical errors*. The claim recites "wherein all management for the first layer 2 device are sent to the source IP address which is assigned to the plane of the layer two device *is part of the virtual local area network*". The limitation should be amended to read: "wherein all management

for the first layer 2 device are sent to the source IP address which is assigned to the plane of the layer two device which is part of the virtual local area network".

Appropriate correction is required.

10. Claim 6 is objected to because of the following informalities: *lack of antecedent basis*. The claim refers to "management *commands*" which was not previously referred to in the parent claim 5.

11. Claim 11 is objected to because of the following informalities: *grammatical errors*. The claim should be amended to read "and only devices which are coupled to the management virtual area network have access to the management functions of the CPU."

Appropriate correction is required.

12. Claim 11 is objected to because of the following informalities: *lack of antecedent basis*. The claim refers to "management virtual area network", which was previously referred to as "management virtual local area network."

Appropriate correction is required.

Claim Rejections - 35 USC § 112

13. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

14. Claims 4 and 5 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per claims 4 and 5, the claims recite limitations regarding a *"layer 2 subnet."* However, those of ordinary skill in the art recognize subnets as being conventionally

associated with layer 3 rather than layer 2. It is unclear if perhaps applicant meant layer 3 subnet rather than *"layer 2 subnet"* as the specification is not consistent in references to the subnet being in layer 2. For instance, *(page 1, lines 25-26)* clearly states "data link layer (layer 2 of the OSI model) subnets," which are later described as including "a number of layer 2 switches networked together, and hosts, such as personal computers or other devices would be connected to the switches" *(page 2, lines 27-29)*. However, subnets are later referred to with regards to the subnet masks designating which subnet a host belongs to *(page 5, lines 6-14),* implying subnets normally associated with layer 3. For the purposes of examination, a "subnet" will be assumed to refer to the layer 3 subnet known conventionally in the art.

As per claim 5, the claim recites the limitation of *"defining a plane of the layer 2 device to be part of the virtual local area network, wherein the plane of the layer 2 device is assigned a source IP address"*. However, those of ordinary skill in the art would recognize a *"plane"* as a logical separation used to classify traffic of packets (control, data, and management). As such, it would not be possible to assign an IP address to such a "plane." However, the specification refers to an embodiment in which "switches in the layer 2 subnets would have **a plane, or port,** which is defined to be included in the MVLAN" (page 6, lines 9-11). For purposes of examination, a "plane" shall be regarded as a "port."

Additionally, claim 5 refers to "the layer 2 device" and "the first layer 2 device" which lack antecedent basis. It is unclear whether "the layer 2 device" refers to the *layer*

2 switch or to the *network device* of claim 1. For the purposes of examination, the "layer 2 device" shall be regarded as the layer 2 switch.

Claim Rejections - 35 USC § 102

15. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

16. Claim 1 is rejected under 35 U.S.C. 102(e) as being anticipated by Phillips et al. *(US Pre-Grant Publication 2004/0210663) (hereinafter Phillips).*

As per claim 1, Phillips teaches a method for providing security, comprising: identifying at least a first port of a the network device, having a first gateway address, as being a management port *(paragraph [0073], the router uses a configured port for dedicated management traffic)*; identifying a group of ports of the network device as being a non-management ports; and filtering out management data packets received on any of the non-management ports *(paragraph [0073], the router isolates management traffic from data traffic, such that all other ports are available for data traffic).*

Claim Rejections - 35 USC § 103

17. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

18. Claims 2-3 are rejected under 35 U.S.C. 103(a) as being unpatentable over Phillips.

As per claim 2, Phillips teaches the method of claim 1 as applied above. Phillips does not explicitly teach the method wherein the filtering out management data packets includes: determining if a destination IP address for a data packet received on one of the group of non-management ports has a destination IP address which corresponds to the gateway address of the first port *(paragraph [0078], the switch can perform filtering with Access Control Lists to deny traffic forwarding to resources)*. However, it is well known and expected in the art to utilize ACLs to filter packets based upon destination IP addresses (as well as type of protocol, source IP address, port, etc.). Examiner takes OFFICIAL NOTICE that it would have been well known and obvious for one of ordinary skill in the art at the time of the invention to isolate management traffic by utilizing ACLs in such a manner in order to easily implement packet filtering based upon destination IP addresses.

As per claim 3, Phillips teaches the method of claim 2 as applied above. Phillips does not explicitly teach the method wherein the filtering out management data packets includes: determining if a data packet received on one of the group of ports utilizes a management protocol; and dropping a data packet where it is determined that a data packet received on one of the group of ports has a destination IP address which corresponds to the gateway address of the first port, and that the data packet utilizes a management protocol. Examiner takes OFFICIAL

NOTICE that it would have been well known and obvious for one of ordinary skill in the art at the time of the invention to isolate management traffic from the non-management ports by using ACL rules in order to provide a simple manner of filtering packets based upon the destination IP address and type of protocol of the packet.

19. Claims 4-5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Phillips in view of Haviland *(Designing High-Performance Campus Intranets with Multilayer Switching, 1998).*

As per claim 4, Phillips teaches the method of claim 1 as applied above. Phillips additionally teaches the method further comprising: defining a virtual local area network to include the first port *(Figure 4).*

Phillips does not teach the method comprising: defining a virtual local area network to include a first layer 2 subnet; allowing access to management functions of the network device only to those hosts which are connected to the first layer 2 subnet.

However, Haviland teaches that a subnet corresponds to a VLAN and wherein a VLAN may map to one or more switches *(page 10, column 2).* Additionally, Haviland teaches designating a VLAN for management traffic whereby policies can be applied with access lists *(page 15, column 1).* As subnets and VLANs correspond to one another, allowing access to hosts connected to the VLAN is analogous to allowing access to hosts connected to the subnet.

It would have been obvious for one of ordinary skill in the art at the time of the invention to combine the teaching of Phillips with that of Haviland in order to define a virtual local area network and subnet such that management functions can only be accessed by hosts connected to

the subnet which contains the designated management port. One would have been motivated to do so as this would allow for access to management traffic and management ports on network devices to be carefully controlled within a management VLAN or a management subnet *(page 15, column 1)*.

As per claim 5, Phillips teaches the method of claim 1, as applied above. Phillips additionally teaches defining a virtual local area network to include the first port *(Figure 4)*.

Phillips does not teach the method comprising: defining a virtual local area network to include a first layer 2 subnet; allowing access to management functions of the network device only to those hosts which are connected to the first layer 2 subnet; connecting a first layer 2 switch to a second port of the group of ports; defining a plane of the layer 2 device to be part of the virtual local area network, wherein the plane of the layer 2 device is assigned a source IP address which corresponds to the gateway address of the first port; and wherein all management for the first layer 2 device are sent to the source IP address which is assigned to the plane of the layer 2 device is part of the virtual local area network.

As noted above, Haviland teaches defining a virtual local area network to include a first layer 2 subnet; allowing access to management functions of the network device only to those hosts which are connected to the first layer 2 subnet. Haviland teaches designating a VLAN for management traffic *(page 15, column 1)*. Therefore, it would have been obvious for one of ordinary skill in the art at the time of the invention to assign a port of a second device (the layer 2 switch) to be part of a management VLAN, such that all management for the second device would be sent to the IP address assigned to the port, such address corresponding to the gateway

address of the management port. One would have been motivated to do so as devices which can be remotely managed can belong to the management VLAN.

20. Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Phillips in view of Haviland, further in view of Sylvest et al. *(US Pre-Grant Publication 2003/0188003) (hereinafter Sylvest)*.

As per claim 6, Phillips and Haviland teach the method of claim 5 as applied above. Phillips and Haviland do not teach the method wherein all management commands have higher priority than all other data packets routed through the network device.

Sylvest teaches management packets having higher priority than the data packets *(paragraph [0029], a prioritizer assures that user data flow cannot re-empt management data flow)*.

It would have been obvious for one of ordinary skill in the art at the time of the invention to combine the teachings of Phillips and Haviland with that of Sylvest in order to provide management packets with higher priority than that of data packets. One would have been motivated to do so as Sylvest teaches that this may prevent the loss of a management packet in the processing of received packets if there are periods of excessive incoming data packets *(paragraph [0029])*.

21. Claims 7-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Phillips in view of Haviland, and further in view of Glenn *(A Summary of DoS/DDoS Prevention, Monitoring and Mitigation Techniques in a Service Provider Environment, 2003)*.

As per claim 7, Phillips teaches the method of claim 1 as applied above. Phillips does not teach the method further including: providing an application specific integrated circuit which is operable to filter out all management data packets received on any of the non-management ports.

However, Haviland teaches ASICs which handle packet forwarding *(page 3)*. Therefore, it would have been obvious for one of ordinary skill in the art at the time of the invention to combine the teaching of Phillips with that of Haviland in order to provide an ASIC which may filter out all management data packets received on any of the non-management ports. One would have been motivated to do so as Glen teaches that ASIC based ACLs perform better than ACLs in software *(page 22)*.

As per claim 8, Phillips teaches the method of claim 1 as applied above. Phillips does not teach the method further including: providing an application specific integrated circuit which is operable to determine if a destination IP address for a data packet received on one of the group of non-management ports is a destination IP address which corresponds to the gateway address of the first port, and to determine if a data packet received on one of the first group of ports utilizes a management protocol, and to drop a data packet where it is determined that a data packet received on one of the group of ports has a destination IP address which corresponds to the gateway address of the first port, and that the data packet utilizes a management protocol.

It is well known and expected in the art to utilize ACLs to filter packets based parameters such as destination IP address and protocol. Therefore, it would have been obvious for one of ordinary skill in the art at the time of the invention to isolate management traffic by utilizing

ACLs in such a manner in order to easily implement packet filtering based upon destination IP address and protocol.

Haviland teaches ASICs which handle packet forwarding *(page 3)*. It would have been obvious for one of ordinary skill in the art at the time of the invention to combine the teaching of Phillips with Haviland in order to provide an ASIC which may filter out management data packets using ACL rules based upon the destination IP address and management protocol. One would have been motivated to do so as Glen teaches that ASIC based ACLs perform better than ACLs in software *(page 22)*.

As per claim 9, Phillips teaches a network device for routing data packets, the network device including: a first port which is defined to be a management port; a group of ports which are not management ports *(paragraph [0073], the router uses a configured port for dedicated management traffic; all other ports are available for data traffic)*; a CPU which is operable to provide management functions, which allow a user to modify the operation of the network device *(Figure 2)*.

Phillips does not teach the device including: an application specific integrated circuit which is operable to deny access to the CPU management functions for all hosts which transmit data packets to the network device through any of the group of ports.

However, Haviland teaches ASICs which handle packet forwarding *(page 3)*. Therefore it would have been obvious for one of ordinary skill in the art at the time of the invention to provide an ASIC which attempt access to management functions through a non-management

port. One would have been motivated to do so as Glenn teaches that ASIC based ACLs perform better than ACLs in software *(page 22)*.

As per claim 10, Phillips and Haviland teach the network device of claim 9, as applied above. Phillips and Haviland additionally teach the device wherein: the first port has a first gateway IP address; wherein the application specific integrated circuit receives data packets, received on each port of the group of ports, and is operable to determine if a data packet received on one the group of ports contains a destination IP address which corresponds to the first gateway IP address.

As noted earlier, Phillips teaches a switch which can perform packet filtering with Access Control Lists *(paragraph [0078]),* and whereby management traffic is isolated from data traffic *(paragraph [0073]);* Haviland teaches that ASICs within routers/switches handle packet forwarding *(page 3)*. It is well known and expected in the art to utilize ACLs to filter packets based parameters such as destination IP address and protocol. Therefore, it would have been obvious for one of ordinary skill in the art at the time of the invention to isolate management traffic by utilizing ACLs in such a manner in order to easily implement packet filtering based upon destination IP address and protocol.

Therefore, Phillips and Haviland as combined above teach the device wherein the application specific integrated circuit is further operable to determine if a data packet received on one of the group of ports utilizes a management protocol; and wherein when it is determined that a data packet received on one of the group of ports is directed to a destination IP address which

corresponds to the first gateway IP address and is in a management protocol, the application specific integrated circuit operates to drop the data packet.

As per claim 11, Phillips and Haviland teach the network device of claim 10 as applied above. Phillips and Haviland as combined above additionally teach the device wherein the first port is defined to be part of a management virtual local area network *(Haviland, page 15, column 1, designating a VLAN for management traffic whereby policies can be applied with access lists)*, and only devices are coupled to the management virtual area network have access to the management functions of the CPU *(Phillips, paragraph [0073], the router isolates management traffic from data traffic)*.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to VIRGINIA HO whose telephone number is 571-270-7309. The examiner can normally be reached on Mon to Thu; 7:30 AM - 5:00 PM (Eastern).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/VIRGINIA HO/
Examiner, Art Unit 2432

/V. H./

/Benjamin E Lanier/
Primary Examiner, Art Unit 2432